REMARKS

Claims 25-61 are in the application of which claims 33 and 36 have been amended to address the indefiniteness objections.

We request reconsideration of the rejections of the claims as being anticipated by Houser et al. '609 or as being unpatentable over Houser in view of Hartman Jr. '166 with or without BOLERO.

Independent Claim 25

In the applicant's view, the subject matter of independent claim 25 is neither taught nor suggested by Houser either alone or in combination with Hartman.

1.) Firstly, claim 25 recites "a method of electronically issuing an electronic negotiable document (END)". The phrase "negotiable document" has a special meaning covering, in particular, bills of lading, cash and bank checks as examples. This is explicitly specified in the first two paragraphs of the application and is reiterated throughout the application. Houser et al. is not concerned with electronic negotiable documents and no skilled person would consider the teachings of Houser to be of any value in dealing with electronic negotiable documents.

To give an example, at the end of the second paragraph of the present application, it is stated, "The main requirement is thus that these documents be unforgeable". By contrast, however, the system described by Houser explicitly teaches away from high security. For example,

"the document configuration management systems provide a very high degree of security and are useful for managing sensitive documents such as time cards in

a corporation. However, document configuration management systems suffer form numerous disadvantages" (Pat. Col. 2, Lines 28-33).

"existing techniques having electronic signature or document configuration management capabilities provide more security than is required...however high confidence verification is unnecessary for the vast majority of transactions..."

"Nonetheless, forgery of any sort is very rare in a business environment. Accordingly security measures which provide a moderate likelihood of detecting deception are effective for deterring forgery or alterations. Therefore, for the vast majority of electronic communications, only a moderate level of security is required..."(Pat. Col. 3, Lines 15-31).

"Accordingly there is a need for electronic data security techniques that are user-friendly, that provide a sufficient degree of security that will deter forgery and alterations, and that can be used in a wide variety of computer systems." (Pat. Col. 3, Lines 42-46).

It can therefore be seen that the systems and techniques described in Houser would be completely unsuitable for electronic negotiable documents.

It is respectfully submitted that a skilled person, looking for techniques which might be employed with electronic negotiable documents would instantly dismiss the teachings of Houser as being unsuitable because they provide only a moderate level of security and rely on the comparative rarity of forgery in a business environment. This is not what is needed, for example, for electronic cash or bank checks.

2.) It is respectively submitted that the Examiner is looking at the teachings of Houser from the point of view of the invention and is reading too much into the document in considering that "tamper-resistant document carrier hardware" is taught or suggested by Houser.

More particularly, nowhere does Houser mention the use of tamper-resistant hardware. Indeed, one of the aims of Houser is to provide techniques which "can be used in a wide variety of computer systems" (Pat. Col. Lines 44-45). Figure 1 to which the Examiner refers, illustrates "a fundamental operation cycle for using the present invention" (Pat. Col. Lines 50-51) and does not teach or imply the presence of any hardware, let alone tamper-resistant hardware. More specifically Houser explicitly teaches that, the "electronic security application may be implemented using a standard computer, such as an IMB PC-compatible computer..."(Pat. Col. 8 Lines 50-53). Houser mentions other hardware examples, for example, "other embodiments might host the application on a different hardware suite, or split portions of the application across multiple pieces of hardware" (Pat. Col. Line 67-Pat. Col. 9, Line 3), but nowhere does Houser teach or suggest that tamper-proof hardware is desirable.

In fact, Houser teaches away from the use of special, tamper-proof hardware since one of the aims of that invention is to provide a system which can be easily used within the structure of "today's highly integrated electronic office tool sets" (Pat. Col. 3, Line 35). Even were the skilled person to have considered the teachings of Houser, it is submitted that to consider employing tamper-resistant hardware to implement the system would negate the primary purpose of Houser, namely a simpler system suitable for stan-

dard hardware which provides "only a moderate level of security" but which is easier to use for the average computer user (Pat. Col. 3, Lines 40-41).

It is therefore submitted that the so-called skilled artisan would have no motivation to modify the teachings of Houser so as to fall within the scope of claim 25.

Claims Dependent Upon Claim 25

It is further submitted that these dependent claims recite additional novel and inventive subject matter neither taught nor disclosed in the prior art.

To take just one example (for the sake of illustration), claim 35 recites the feature of "a counter for storing a serial number representative of the number of times the END has been negotiated". This feature is neither taught nor suggested in either Houser or Hartman. Although Houser refers to a serial number-"a serial number that is unique for each embedded security object" (Pat. Col. 4, Lines 17-18), and a "serial number generator may be provided for generating a unique serial number..." (Pat. Col. 4, Lines 35-36), this serial number is "unique". By contrast, the serial number feature recited in claim 35 represents a number of times the END has been negotiated. This prevents the owner an END selling it twice to two different entities (see the final six lines of page 9 of the present application and the first two lines of page 10). Clearly where, for example, an electronic negotiable document represents cash, the owner cannot be permitted to give the cash away twice (which would effectively double their money), but this problem does not even arise in the context of the Houser system and, instead, although a serial number is mentioned, this is "unique for each embedded security object"-and is therefore not changed-so cannot act as a counter to perform the function in claim 35.

Independent Claim 36

1.) The same points as made above in connection with claim 25 can also be made in connection with claim 36: Houser is not concerned with "electronic negotiable documents", nor does Houser either teach or suggest or give any motivation for the use of "tamper-resistant document carrier hardware"-as recited in claim 36.

2.) The assertion of the Examiner that the application background section teaches that it is well known for data for a seller's document carrier to be encrypted and so forth is respectfully contested as this is based upon a misreading of the text at application page 3. The applicant states, "It is known to provide an encryption technique...", then going on to describe and give references for the Diffie Hellman, RSA and DSA techniques. However, the final sentence of this paragraph describes how these techniques can be used, not what is known. It is respectfully submitted that the language of this paragraph is clear and only acknowledges that "an encryption technique which ensures uniqueness in the transfer of data between two devices" is known together with the examples of such a technique which are given. The reference to "data from a seller's document carrier, for example, can be encrypted using the public key..." is an application of the previously described encryption technique which, on a factual reading of the text of the application, is not acknowledged to be known (still less "well known").

3.) The Examiner in rejecting claim 36 states "Houser does not explicitly teach encryption status flag", but the claim language does not refer to an encryption status flag. Rather, the claim recites a "negotiability status flag" which is "indicative of whether the

END is currently negotiable...", and which has "negotiable" and "non-negotiable" settings.

In other words, a negotiability status flag differs from an encryption status flag in that the negotiability status flag allows a buyer to determine whether or not an END is negotiable, and hence whether or not the buyer proceeds with a negotiation, without contacting a trusted third party. Using the negotiability status flag, it is possible to establish "mutual recognition between the seller and buyer" and to verify "in the seller's document carrier hardware that the negotiability status flag is 'negotiable' and aborting the negotiation if not". This overcomes a disadvantage inherent in the prior art that a trusted third party is required to guarantee that an electronic document is negotiable.

A "serial number counter indicative of the number of times that the END has been negotiated since issue" allows a buyer who was previously the seller of an END to receive the END back again, but only as a result of a genuine transaction. This is done by "verifying in the seller's document carrier hardware that the END, if it has been stored previously in that document carrier hardware, has a different counter value this time and is therefore negotiable.

Consider the example of when the END comprises electronic cash which is to be passed from A to B. Once the negotiable document (in this example, cash) has been passed from A to B, A's document carrier hardware has it's negotiability status flag set to non-negotiable, and the document carrier hardware of the recipient B, has the negotiability status flag set to negotiable. This means that the electronic negotiable document (in

this example, cash) is, at any one time, the property of a particular user (see the second paragraph of the present application).

The system described by Hartman is not concerned with electronic negotiable documents and neither teaches nor suggests a "negotiability status flag" as claimed. As the Examiner points out, Hartman does describe an encryption status flag to indicate, "whether the memory segment is encrypted or non-encrypted" (Pat. Col. 6, Lines 1-3), but this is not a "negotiability status flag" and does not have the claimed properties of that flag.

Even if a skilled person were to attempt to use the teachings of Hartman in the system of Houser there would be nothing to either teach or suggest the implementation of a negotiability status flag as claimed. In more detail, the Examiner refers to the text at Pat. Col 8, Lines 37-59 of Hartman, which recites that the flag indicates an encrypted status, and refers to encryption control means responsive to a state of the flag in perfom-ring its function. Even if the skilled person found some motivation for combining the teachings of Houser and Hartman, the combination would merely teach use of a system with encrypted and non-encrypted data and encryption control means responsive to a state of an encrypted status flag. This would not be a "negotiability status flag" as recited in claim 36-which is entirely consistent with the fact that neither Houser nor Hartman mention or are concerned in any way with electronic negotiable documents.

Independent Claim 37

Similar points can be made here to those made in relation to claim 36, above. In claim 37, however, a "counter indicative of the number of times that the END [electronic

negotiable document] has been negotiated since issue" is recited. Again, this neither taught nor suggested in either Houser or Hartman. The Examiner is also referred to the comments made above under the heading "Claims Dependent Upon Claim 25".

Claims Dependent Upon Claim 36 or Claim 37

These claims recite additional, novel and inventive subject matter. For example, claims 38 and 39 each refer to a certificate being installed on a document carrier hardware. The context of the application makes it completely clear that this certificate is part of the public-private key infrastructure, generally issued by a trusted party called the "Certification Authority", CA (see the paragraphs at the top and bottom of page 6 of the present application). There is no reference anywhere in Houser to a "Certificate", and a certificate appears to be an example of a technique which provides "more security than is required", which Houser is deliberately trying to avoid. There would, therefore, be no motivation to try to include such a certificate in the system of Houser.

In another example, with reference to claims 54 and 55 the claim language here refers to recovering the negotiation of an END (electronic negotiable document). However, the prior art does not recognize the existence of such a problem, in particular in respect of tamper-resistant document carrier hardware (as recited in claims 36 and 37 upon which claims 54 and 55, respectively, depend): the features of these claims address the problem of how to ensure that an electronic negotiable document (which has a value) can be recovered for the rightful owner if a tamper resistant box breaks down.

Independent Claim 60

The Examiner has rejected this claim as being anticipated by BOLERO (Article I). In doing so, the Examiner has ignored the steps "in which the buyer splits the END electronically into two or more parts and then negotiates those parts separately to one or more further buyers" recited in claim 60. This feature is neither taught nor hinted at in BOLERO.

Dependent claim 61 further recites that "each part is subjected to the digital signature of the document carrier hardware of the buyer which effects the splitting". Again, there is no hint or suggestion of this in the cited Article.

Regarding BOLERO, the claimed invention was introduced as a radical alternative to BOLERO (the security architecture of which was actually designed by present applicant). Another important difference from the present invention is that Bolero requires a trusted third party to be involved (as a witness) in each separate transaction (to prevent double-spending).

Accordingly and for the foregoing reasons, claims 25-61 should be allowed and we request reconsideration to that end.

Please charge any additional fee occasioned by this paper to our Deposit Account No. 03-1237.

Respectfully submitted,

John F. McKenna
Reg. No. 20,912
CESARI AND MCKENNA, LLP
88 Black Falcon Avenue
Boston, MA 02210-2414
(617) 951-2500